

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Cancelled).

2. (Currently Amended) A smartcard according to claim 3[[1]] wherein said [[the]] secondary memory device is a FLASH ROM.

3. (Currently Amended) A smartcard ~~according to claim 1 or 2 comprising:
a substrate having a smartcard chip thereon; and~~
~~a secondary memory device on said substrate and operatively connected to the smartcard
chip,~~

wherein [[the]] said secondary memory device is configured to store capable of storing a plurality of pages of data, each page having associated with it a unique sequence number, the sequence number being stored separately from the data page so that when the page is to be read, the sequence number retrieved with the page can be compared with the stored sequence number to authenticate the page.

4. (Original) A smartcard according to claim 3 wherein the stored sequence number is stored in the smartcard chip.

5. (Currently Amended) A smartcard according to claim 3 wherein some of the stored sequence numbers are stored in at least one page of the plurality of pages of data stored on the secondary memory device, the sequence number for that at least one page being stored in the smartcard chip.

6. (Currently Amended) A smartcard according to claim 3 wherein the sequence numbers are XOR'd to produce a digest or HASH which is stored in a the smartcard EEPROM.

7. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 5-wherein the sequence number associated with a particular page of data is changed each time the page is modified or updated.

8. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 6-wherein the sequence number for each page of data is set initially at a randomly generated value.

9. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 8-wherein each page contains a copy of its page number.

10. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 9-wherein the data in each page is encrypted.

11. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 10-wherein ~~each~~ page data integrity is protected with a cryptographic MAC.

12. (Currently Amended) A smartcard according to ~~any of~~ claim[[s]] 3 to 11-wherein the data in each page is encrypted, and page data integrity is protected with a cryptographic MAC, wherein each page encryption and cryptographic MAC [[is]] are performed using a page and chip unique key.

13. (New) A smartcard comprising:
a substrate having a smartcard chip thereon; and
a secondary memory device on said substrate and operatively connected to the smartcard chip,

wherein said secondary memory device is configured to store a plurality of pages of data, each page having associated with it a unique sequence number, the sequence number being stored separately from the page so that when the page is to be read, the sequence number retrieved with the page can be compared with the stored sequence number to authenticate the page; and

wherein the sequence number associated with a particular page of data is changed each time the page is modified or updated.

14. (New) A smartcard according to claim 13 wherein the sequence number for each page of data is set initially at a randomly generated value.

15. (New) A smartcard according to claim 13 wherein each page contains a copy of its page number.

16. (New) A smartcard according to claim 13 wherein the date in each page is encrypted.

17. (New) A smartcard according to claim 13 wherein each page data integrity is protected with a cryptographic MAC.

18. (New) A smartcard according to claim 13 wherein the data in each page is encrypted, and page data integrity is protected with a cryptographic MAC, wherein page encryption and cryptographic MAC are performed using a page and chip unique key.

19. (New) A smartcard according to claim 13 wherein said secondary memory device is a FLASH ROM.

20. (New) A smartcard comprising:

a substrate having a smartcard chip thereon; and

a secondary memory device on said substrate and operatively connected to the smartcard chip,

wherein said secondary memory device is capable of storing a plurality of pages of data, each having associated with it a unique sequence number, the sequence number being stored separated from the data page so that when the page is to be read, the sequence number retrieved with the page can be compared with the stored sequence number to authenticate the page; and

wherein the sequence number for each page of data is a randomly generated value.

21. (New) A smartcard according to claim 20 wherein the sequence number associated with a particular page of data is changed to another randomly generated value each time the page is modified or updated.